

Draft, June 17, 2016

ISOMETRY GROUPS OF COMBINATORIAL CODES

SERHII DYSHKO

ABSTRACT. Two isometry groups of combinatorial codes are described: the group of automorphisms and the group of monomial automorphisms, which is the group of those automorphisms that extend to monomial maps. Unlike the case of classical linear codes, where these groups are the same, it is shown that for combinatorial codes the groups can be arbitrary different. Particularly, there exist codes with the full automorphism group and the trivial monomial automorphism group. In the paper the two groups are characterized and codes with predefined isometry groups are constructed.

1. INTRODUCTION

An automorphism group of a classical linear code is the group of those linear bijections from the code to itself that preserve the Hamming distance. MacWilliams proved in her Ph.D. thesis [8] that each linear Hamming isometry of a classical linear code extends to a monomial map, i.e., it acts by permutation of coordinates and multiplication of coordinates by nonzero scalars. Consequently, each automorphism of a linear code extends to a monomial map.

As it was shown in numerous papers [4, 6, 13], for linear codes over module alphabets an analogue of the MacWilliams Extension Theorem does not hold in general. This means that there may exist codes with automorphisms that do not extend to monomial maps. In the context of combinatorial codes, i.e., codes without any algebraic structure, the situation is similar, see [1, 7, 9].

For the case of non-classical codes, along with the automorphism group of a code there is observed the subgroup of those automorphisms that extend to monomial maps. As was mentioned above, unlike the case of classical linear codes, the two groups may not be the same.

In [11] Wood investigated the question of how different the two groups of a linear code over a matrix module alphabet can be. He showed, under certain assumptions, that there exists a linear code over a matrix module alphabet with predefined group of automorphism and group of monomial automorphism. In this paper we prove a similar statement for combinatorial codes.

2. PRELIMINARIES

Let A be a finite set, called an *alphabet*, and let n be a positive integer. The *Hamming distance* is a function $\rho_H : A^n \times A^n \rightarrow \{0, \dots, n\}$, defined as, for $a, b \in A^n$,

$$\rho_H(a, b) := |\{k \mid a_k \neq b_k\}|.$$

The set A^n equipped with the Hamming distance is a metric space called a *Hamming space*. A *code* C is a subset of the Hamming space A^n . The elements of C are called *codewords*.

A map $f : C \rightarrow A^n$ is called a *Hamming isometry* if for each two codewords $a, b \in C$, $\rho_H(a, b) = \rho_H(f(a), f(b))$, i.e., the map f preserves the Hamming distance.

For a finite set X , let $\mathfrak{S}(X)$ denote the symmetric group on X . Denote $\mathfrak{S}_n = \mathfrak{S}(\{1, \dots, n\})$, where n is a positive integer.

A map $h : A^n \rightarrow A^n$ is called *monomial* if there exists a permutation $\pi \in \mathfrak{S}_n$ and permutations $\sigma_1, \dots, \sigma_n \in \mathfrak{S}(A)$ such that for each $a \in A^n$,

$$h(a) = (\sigma_1(a_{\pi(1)}), \dots, \sigma_n(a_{\pi(n)})).$$

Let $C \subseteq A^n$ be a code with $m \geq 3$ codewords. Consider the set $M = \{1, \dots, m\}$, called the *set of messages*, and consider an *encoding map* $\lambda : M \rightarrow A^n$ of the code C , i.e., an injective map such that $\lambda(M) = C$. For every $g \in \mathfrak{S}(M)$ the map $\lambda g \lambda^{-1} : C \rightarrow C$ is a well-defined bijection.

Define the *group of automorphisms* of C ,

$$\text{Iso}(C) := \{g \in \mathfrak{S}(M) \mid \lambda g \lambda^{-1} \text{ is a Hamming isometry}\},$$

and the *group of monomial automorphisms* of C ,

$$\text{Mon}(C) := \{g \in \text{Iso}(C) \mid \lambda g \lambda^{-1} \text{ extends to a monomial map}\}.$$

Remark 1. In coding theory the group $\text{Mon}^*(C)$ of those monomial maps that preserve C is often used. The set of all monomial maps of A^n form a group, which is isomorphic to the wreath product $\mathfrak{S}_n \wr \mathfrak{S}(A)$, see [5, Section 2.6]. Note that $\text{Mon}(C)$ and $\text{Mon}^*(C)$ are different objects: $\text{Mon}(C)$ is a subgroup of $\mathfrak{S}(M)$ and $\text{Mon}^*(C)$ is a subgroup of the full group of monomial maps. However, there exists a connection. For a monomial map $h \in \text{Mon}^*(C)$ the map $\lambda^{-1} h \lambda$ is in $\text{Iso}(C)$. By defining the map $\text{restr} : \text{Mon}^*(C) \rightarrow \text{Iso}(C)$, $h \mapsto \lambda^{-1} h \lambda$, we have the equality of groups $\text{Mon}(C) = \text{restr}(\text{Mon}^*(C))$. The groups $\text{Mon}(C)$ and $\text{Mon}^*(C)$ are isomorphic unless the homomorphism restr has a nontrivial kernel. The last holds if and only if the code has two columns that differ by a permutation of the alphabet.

In [2] and in [3, Theorem 1] the equality of the groups $\text{Iso}(A^n)$ and $\text{Mon}(A^n)$ was proven. However, in general, for codes in A^n the equality of groups does not hold.

Example 1. Suppose $A = \{0, 1\}$, $M = \{1, \dots, 5\}$. Consider the code C of cardinality 5 in A^4 ,

$$C = \{(0, 0, 0, 0), (1, 1, 0, 0), (1, 0, 1, 0), (1, 0, 0, 1), (0, 1, 1, 0)\},$$

where the encoding $\lambda : M \rightarrow C$ is given in the presented order. The group $\text{Iso}(C) < \mathfrak{S}(M)$ is generated by cycles $(1, 2)$, $(1, 2, 3)$ and $(4, 5)$ and has 12 elements. From the other side, $\text{Mon}(C)$ is a subgroup of $\text{Iso}(C)$ generated by permutations $(1, 2)$ and $(1, 2, 3)$. For example, denoting $g_0 = (4, 5) \in \text{Iso}(C)$, the map $\lambda g_0 \lambda^{-1}$ is an automorphism of C that does not extend to a monomial map,

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \xrightarrow{\lambda g_0 \lambda^{-1}} \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}.$$

Indeed, one can easily check that $\lambda g_0 \lambda^{-1} : C \rightarrow C$ is a Hamming isometry. Also, the fourth column from the right hand side has equal first four elements, but there is no such column from the left hand side. Hence, the code automorphism $\lambda g_0 \lambda^{-1}$ does not extend to a monomial map.

Therefore, $\text{Mon}(C) \neq \text{Iso}(C)$. Note that the group $\text{Mon}^*(C)$ is generated by two elements. One acts by swapping the second and the third column of C and another acts by inverting the symbols in the first two columns and then swapping the first two columns. Both groups $\text{Mon}^*(C)$ and $\text{Mon}(C)$ have 6 elements and are isomorphic to the symmetric group \mathfrak{S}_3 .

There exist more complex examples. Recall that a code $C \subseteq A^n$ is an (n, K, d) q -ary code if it has cardinality K , minimum distance d and the alphabet has q elements. According to [9], if C is $(q, q^2, q-1)$ or $(q+1, q^2, q)$ q -ary MDS code with $q \neq 2$, then $|\text{Iso}(C)| > |\text{Mon}(C)|$, and thus $\text{Iso}(C) \neq \text{Mon}(C)$. The same holds, for example, for $(q, (q-1)^2, q-1)$ q -ary equidistant codes, where $q \geq 5$ and both q and $q-1$ are prime powers (see [7]).

The main result of this paper is given in the next section.

3. MAIN RESULT

Let G be a group acting on a set X . We say that a subgroup $H \leq G$ is *closed under the action on X* if H consists of all those elements in G that preserve the orbits of H . To be precise, we say that H is closed under the action on X if,

$$\forall g \in G, \forall O \in X/H, \quad g(O) = O \Rightarrow g \in H,$$

where X/H is the set of orbits of H acting on X . A similar definition of a closed group and a definition of a closure of a group were introduced by Wielandt in his 2-closure theory (see [10]). More results on the closure can be found in [5, Section 2.4] and [14].

Let q denote the cardinality of the alphabet A , $q \geq 2$. Consider the set \mathcal{P} of all the partitions of the set M that have at most q classes,

$$\mathcal{P} := \{ \{c_1, \dots, c_t\} \mid c_1 \sqcup \dots \sqcup c_t = M, \quad t \leq q \},$$

where $c_i \subseteq M$, for $i \in \{1, \dots, t\}$, and \sqcup denotes the disjoint union of sets.

The canonical action of the group $\mathfrak{S}(M)$ on the set \mathcal{P} is defined in the following way, for $g \in \mathfrak{S}(M)$, for $\alpha = \{c_1, \dots, c_t\} \in \mathcal{P}$,

$$g(\alpha) := \{g(c_1), \dots, g(c_t)\}.$$

In \mathcal{P} we distinguish a subset

$$\mathcal{P}_2 := \left\{ \{ \{i, j\}, \{M \setminus \{i, j\}\} \} \mid \{i, j\} \subset M \right\}.$$

Since each partition in \mathcal{P}_2 has two classes, which is not greater than q , $\mathcal{P}_2 \subset \mathcal{P}$. The group $\mathfrak{S}(M)$ naturally acts on \mathcal{P}_2 and $\mathcal{P} \setminus \mathcal{P}_2$.

Theorem 1. *Let A be a finite set alphabet of cardinality $q \geq 2$ and let C be a code over the alphabet A of cardinality $m \geq 5$ or $m = 3$. The following statements hold.*

- (i) *The group $\text{Iso}(C) \leq \mathfrak{S}(M)$ is closed under the action on \mathcal{P}_2 .*
- (ii) *The group $\text{Mon}(C)$ is equal to an intersection of $\text{Iso}(C)$ with a subgroup of $\mathfrak{S}(M)$ closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$.*
- (iii) *For each subgroup $H_1 \leq \mathfrak{S}(M)$ that is closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$, for each subgroup $H_2 \leq \mathfrak{S}(M)$ that is closed under the action on \mathcal{P}_2 , there exists a code C of cardinality $m \geq 5$ such that*

$$\text{Mon}(C) = H_1 \cap \text{Iso}(C) \quad \text{and} \quad \text{Iso}(C) = H_2.$$

From the fact that, for $m \geq 5$, the trivial subgroup $\{e\}$ and the full group $\mathfrak{S}(M)$ are closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$ and \mathcal{P}_2 respectively, we get the first corollary.

Corollary 1. *For every integer $m \geq 5$, there exists a code C of cardinality m with the maximal group $\text{Iso}(C) = \mathfrak{S}(M)$ and the minimal group $\text{Mon}(C) = \{e\}$.*

By using Theorem 1 (iii) with $H_1 = \mathfrak{S}(M)$, which is closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$, we get the second corollary.

Corollary 2. *For every integer $m \geq 5$ or $m = 3$, for each subgroup $H \leq \mathfrak{S}(M)$ that is closed under the action on \mathcal{P}_2 , there exists a code C of cardinality m such that the groups $\text{Mon}(C)$ and $\text{Iso}(C)$ coincide and are both equal to H .*

Example 2. For $m = 5$ and $q = 2$, consider the code C of the following form.

0	0	1	2	3	4	6	5	4	3	4	3	2	2	1	0
0	1	0	0	0	0	1	1	1	1	0	0	0	0	0	0
0	0	1	0	0	0	1	0	0	0	1	1	1	0	0	0
0	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0
0	0	0	0	1	0	0	0	1	0	0	1	0	1	0	1
0	0	0	0	0	1	0	0	0	1	0	0	1	0	1	1

The numbers over the header line represent the number of occurrences of the column under the line in the code. For instance, in this example, the third column appears once in the code, the fourth column appears twice in the code and the second column does not appear anywhere in the code.

We indicated several columns that does not appear in the code for the completeness. In fact, all possible columns (up to a permutation of the alphabet) are presented in the table. The vertical lines separate the columns with different numbers of 1s.

The code C is a $(40, 5, 22)$ equidistant binary code with the maximal automorphism group $\text{Iso}(C) = \mathfrak{S}(M)$ and the minimal monomial automorphism group $\text{Mon}(C) = \{e\}$.

Remark 2. In general, for $m \geq 5$, there is no direct relation between the subgroups of $\mathfrak{S}(M)$ closed under the action on \mathcal{P}_2 and $\mathcal{P} \setminus \mathcal{P}_2$. There exists a subgroup that is closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$ but not closed under the action on \mathcal{P}_2 . For example, if $m = 5$, $q = 3$ and the group is $G = \langle (1, 2)(3, 4), (1, 2)(3, 5) \rangle < \mathfrak{S}_5$. There also exists a subgroup that is closed under the action on \mathcal{P}_2 but not closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$. Consider $m = 5$, $q = 2$ and $G = \langle (1, 2)(3, 4) \rangle < \mathfrak{S}_5$.

For codes with $m = 4$ codewords the statement of the theorem is not correct in general and needs to be refined. This case is observed in Appendix A.

4. MULTIPLICITY FUNCTION

For sets X, Y , let $F(X, Y)$ denote the set of all maps from X to Y . Consider the map $\Psi : F(M, A) \rightarrow \mathcal{P}$,

$$x \mapsto \Psi(x) := \{x^{-1}(a) \mid a \in A\} \setminus \{\emptyset\}.$$

The number of classes in $\Psi(x)$ is at most $|A| = q$, so $\Psi(x) \in \mathcal{P}$ and hence the map is defined.

Recall that $\lambda : M \rightarrow A^n$ is an encoding map of C . Let $\lambda_k : M \rightarrow A$ denote the projection of λ on k th coordinate for $k \in \{1, \dots, n\}$. Define the *multiplicity function* $\eta_\lambda \in F(\mathcal{P}, \mathbb{Q})$, as follows, for $\alpha \in \mathcal{P}$,

$$\eta_\lambda(\alpha) := |\{k \mid \Psi(\lambda_k) = \alpha\}|.$$

Proposition 1. *For every non-zero function $\eta \in F(\mathcal{P}, \mathbb{Q})$ with nonnegative integer values there exist a positive integer n and a map $\lambda : M \rightarrow A^n$, such that $\eta_\lambda = \eta$.*

Proof. Define $n = \sum_{\alpha \in \mathcal{P}} \eta(\alpha)$ and let $\alpha_1, \dots, \alpha_n \in \mathcal{P}$ be the n -tuple of partitions such that for all $\alpha \in \mathcal{P}$,

$$\eta(\alpha) = |\{k \mid \alpha = \alpha_k\}|.$$

Enumerate the elements of the alphabet $A = \{a_1, \dots, a_q\}$ and fix $k \in \{1, \dots, n\}$. Let $\alpha_k = \{c_1, \dots, c_t\}$, for some $t \leq q$. Define the map $\lambda_k \in F(M, A)$ as

$$\forall i \in \{1, \dots, t\}, \forall j \in c_i, \quad \lambda_k(j) = a_i.$$

It is easily seen that $\Psi(\lambda_k) = \alpha_k$. Define $\lambda = (\lambda_1, \dots, \lambda_n) : M \rightarrow A^n$. Then, for all $\alpha \in \mathcal{P}$, $\eta_\lambda(\alpha) = |\{k \mid \Psi(\lambda_k) = \alpha\}| = |\{k \mid \alpha_k = \alpha\}| = \eta(\alpha)$. \square

5. EXTENSION CRITERION AND STABILIZERS

Let \mathcal{O} denote the set of pairs of elements of M ,

$$\mathcal{O} := \{\{i, j\} \mid \{i, j\} \subset M\}.$$

The group $\mathfrak{S}(M)$ acts on \mathcal{O} in the following way, for $g \in \mathfrak{S}(M)$,

$$g(\{i, j\}) := \{g(i), g(j)\}.$$

Consider the action of $\mathfrak{S}(M)$ on the vector spaces $F(\mathcal{P}, \mathbb{Q})$ and $F(\mathcal{O}, \mathbb{Q})$, so that, for $g \in \mathfrak{S}(M)$, for $\eta \in F(\mathcal{P}, \mathbb{Q})$ and $\alpha \in \mathcal{P}$,

$$g(\eta)(\alpha) := \eta(g^{-1}(\alpha)),$$

and for $x \in F(\mathcal{O}, \mathbb{Q})$ and $p \in \mathcal{O}$,

$$g(x)(p) := x(g^{-1}(p)).$$

The group $\mathfrak{S}(M)$ acts on the vector spaces by automorphisms, i.e., a map $\phi : V \rightarrow V$, associated to the action of g on V , is a \mathbb{Q} -linear bijection, where V is either $F(\mathcal{P}, \mathbb{Q})$ or $F(\mathcal{O}, \mathbb{Q})$.

For $\alpha \in \mathcal{P}$ and $p = \{i, j\} \in \mathcal{O}$, define the function $\Delta_\alpha \in F(\mathcal{O}, \mathbb{Q})$ as

$$\Delta_\alpha(p) := \begin{cases} 0, & \text{if } i \text{ and } j \text{ belong to the same class in } \alpha; \\ 1, & \text{otherwise.} \end{cases}$$

Consider the \mathbb{Q} -linear map,

$$W : F(\mathcal{P}, \mathbb{Q}) \rightarrow F(\mathcal{O}, \mathbb{Q}), \quad W(\eta)(p) := \sum_{\alpha \in \mathcal{P}} \eta(\alpha) \Delta_\alpha(p),$$

where $\eta \in F(\mathcal{P}, \mathbb{Q})$, $p \in \mathcal{O}$. A similar map was observed in [12, 13].

Proposition 2. *A map $f : C \rightarrow A^n$ is a Hamming isometry if and only if $W(\eta_\lambda) = W(\eta_{f\lambda})$. The map f extends to a monomial map if and only if $\eta_\lambda = \eta_{f\lambda}$.*

Proof. Calculate the Hamming distance, for all $p = \{i, j\} \in \mathcal{O}$,

$$\begin{aligned} \rho_H(\lambda(i), \lambda(j)) &= |\{k \mid \lambda_k(i) \neq \lambda_k(j)\}| \\ &= |\{k \mid \Delta_{\Psi(\lambda_k)}(p) = 1\}| \\ &= \sum_{\alpha \in \mathcal{P}} |\{k \mid \Psi(\lambda_k) = \alpha\}| \Delta_\alpha(p) \\ &= \sum_{\alpha \in \mathcal{P}} \eta_\lambda(\alpha) \Delta_\alpha(p) = W(\eta_\lambda)(p). \end{aligned}$$

The map f is a Hamming isometry if and only if for all $\{i, j\} \subset M$,

$$\rho_H(\lambda(i), \lambda(j)) = \rho_H(f\lambda(i), f\lambda(j)),$$

which is equivalent to the equality $W(\eta_\lambda) = W(\eta_{f\lambda})$.

The map f extends to a monomial map if and only if there exist a permutation $\pi \in \mathfrak{S}_n$ and permutations $\sigma_1, \dots, \sigma_n \in \mathfrak{S}(A)$ such that $f\lambda_k = \sigma_k \lambda_{\pi(k)}$, for all $k \in \{1, \dots, n\}$.

It is an easy exercise to verify that $\Psi(x) = \Psi(y)$ for two maps $x, y \in F(M, A)$, if and only if there exists a permutation $\sigma \in \mathfrak{S}(A)$ such that $\sigma x = y$.

If f extends to a monomial map, then for all $\alpha \in \mathcal{P}$,

$$\begin{aligned} \eta_{f\lambda}(\alpha) &= |\{k \mid \Psi(f\lambda_k) = \alpha\}| \\ &= |\{k \mid \Psi(\sigma_k \lambda_{\pi(k)}) = \alpha\}| \\ &= |\{k \mid \Psi(\lambda_{\pi(k)}) = \alpha\}| = \eta_\lambda(\alpha). \end{aligned}$$

Conversely, let $\eta_{f\lambda} = \eta_\lambda$. Then for all $\alpha \in \mathcal{P}$ the cardinality of sets $X_\alpha = \{k \mid \Psi(\lambda_k) = \alpha\}$ and $Y_\alpha = \{k \mid \Psi(f\lambda_k) = \alpha\}$ are equal. The set $\{1, \dots, n\}$ is then a disjoint union of the subsets X_α for $\alpha \in \mathcal{P}$. It is also equal to a disjoint union of the subsets Y_α for $\alpha \in \mathcal{P}$. Thus, there exists $\pi \in \mathfrak{S}_n$ such that for all $\alpha \in \mathcal{P}$, $\pi(X_\alpha) = Y_\alpha$. Therefore, for all $k \in \{1, \dots, n\}$, $\Psi(\lambda_{\pi(k)}) = \Psi(f\lambda_k)$. From this, for every $k \in \{1, \dots, n\}$ there exists $\sigma_k \in \mathfrak{S}(A)$ such that $\sigma_k \lambda_{\pi(k)} = f\lambda_k$, which means that f extends to a monomial map. \square

For a map $\eta \in F(\mathcal{P}, \mathbb{Q})$ define two stabilizers,

$$\begin{aligned} \text{Stab}(\eta) &:= \{g \in \mathfrak{S}(M) \mid g(\eta) = \eta\}, \\ \text{Stab}_W(\eta) &:= \{g \in \mathfrak{S}(M) \mid W(g(\eta)) = W(\eta)\}. \end{aligned}$$

Proposition 3. *If C is a code with an encoding map $\lambda : M \rightarrow A^n$, then*

$$\text{Mon}(C) = \text{Stab}(\eta_\lambda), \quad \text{Iso}(C) = \text{Stab}_W(\eta_\lambda).$$

Proof. For all $g \in \mathfrak{S}(M)$, for all $\alpha \in \mathcal{P}$,

$$\eta_{\lambda g}(\alpha) = |\{k \mid \Psi(\lambda_k g) = \alpha\}| = |\{k \mid \Psi(\lambda_k) = g^{-1}(\alpha)\}| = \eta_\lambda(g^{-1}(\alpha)) = g(\eta_\lambda)(\alpha).$$

The statement of the proposition follows directly from Proposition 2 by substituting $\lambda g \lambda^{-1}$ in place of f . \square

6. TWO MATRICES

For two pairs $p, t \in \mathcal{O}$, the intersection $p \cap t \subset M$ can have at most 2 elements. On \mathcal{O} fix an order. Let B be the $|\mathcal{O}| \times |\mathcal{O}|$ matrix defined over \mathbb{Q} and indexed by the elements of \mathcal{O} . For $p, t \in \mathcal{O}$,

$$B_{p,t} := \begin{cases} 1, & \text{if } |p \cap t| = 1; \\ 0, & \text{if } |p \cap t| \neq 1. \end{cases}$$

Let $m \geq 5$ or $m = 3$. Define the $|\mathcal{O}| \times |\mathcal{O}|$ matrix D as follows, for $p, t \in \mathcal{O}$,

$$2(m-2)(m-4) \times D_{p,t} := \begin{cases} -m^2 + 8m - 14, & \text{if } |p \cap t| = 2 \text{ (} \iff p = t \text{)}; \\ m - 4, & \text{if } |p \cap t| = 1; \\ -2, & \text{if } |p \cap t| = 0 \text{ (} \iff p \cap t = \emptyset \text{)}. \end{cases}$$

Lemma 1. *If $m \geq 5$ or $m = 3$, then $BD = DB = I$, where I is the identity $|\mathcal{O}| \times |\mathcal{O}|$ matrix.*

Proof. For $p, t \in \mathcal{O}$,

$$(BD)_{p,t} = \sum_{r \in \mathcal{O}} B_{p,r} D_{r,t} = B_{p,t} D_{t,t} + \sum_{\substack{|r \cap p|=1 \\ |r \cap t|=1}} D_{r,t} + \sum_{\substack{|r \cap p|=1 \\ |r \cap t|=0}} D_{r,t}.$$

If $p = t$, then

$$(BD)_{p,p} = 0 + \sum_{|r \cap p|=1} D_{r,p} + 0 = \frac{1}{2(m-2)} |\{r \in \mathcal{O} \mid |r \cap p| = 1\}| = 1.$$

If $|p \cap t| = 1$, then

$$\begin{aligned} (BD)_{p,t} &= \frac{-m^2 + 8m - 14}{2(m-2)(m-4)} + \frac{1}{2(m-2)} |\{r \in \mathcal{O} \mid |r \cap p| = 1; |r \cap t| = 1\}| \\ &\quad + \frac{-1}{(m-2)(m-4)} |\{r \in \mathcal{O} \mid |r \cap p| = 1; |p \cap t| = 0\}| \\ &= \frac{-m^2 + 8m - 14}{2(m-2)(m-4)} + \frac{(m-4)}{2(m-2)(m-4)} (m-2) + \frac{-2}{2(m-2)(m-4)} (m-3) = 0. \end{aligned}$$

If $|p \cap t| = 0$, then

$$\begin{aligned} (BD)_{p,t} &= 0 + \frac{1}{2(m-2)} |\{r \in \mathcal{O} \mid |r \cap p| = 1; |r \cap t| = 1\}| \\ &\quad + \frac{-1}{(m-2)(m-4)} |\{r \in \mathcal{O} \mid |r \cap p| = 1; |r \cap t| = 0\}| \\ &= \frac{4}{2(m-2)} + \frac{-2}{2(m-2)(m-4)} 2(m-4) = 0. \end{aligned}$$

Hence, $BD = I$, the matrices B and D are invertible and $B^{-1} = D$. \square

7. PROPERTIES OF THE MAP W

For a partition $\alpha \in \mathcal{P}$ let $\mathbb{1}_\alpha \in F(\mathcal{P}, \mathbb{Q})$ be the map defined as follows, for $\beta \in \mathcal{P}$,

$$\mathbb{1}_\alpha(\beta) := \begin{cases} 1, & \text{if } \beta = \alpha; \\ 0, & \text{if } \beta \neq \alpha. \end{cases}$$

Note that, for $\alpha \in \mathcal{P}$, for $p \in \mathcal{O}$,

$$(1) \quad W(\mathbb{1}_\alpha)(p) = \sum_{\beta \in \mathcal{P}} \mathbb{1}_\beta(\alpha) \Delta_\beta(p) = \Delta_\alpha(p).$$

From now we assume that $m \geq 5$ or $m = 3$. For every map $x \in F(\mathcal{O}, \mathbb{Q})$ define the map in $F(\mathcal{P}, \mathbb{Q})$,

$$\xi_x := \sum_{r \in \mathcal{O}} x(r) \sum_{p \in \mathcal{O}} D_{r,p} \mathbb{1}_{\{p, M \setminus p\}},$$

where D is the matrix defined previously. Using Lemma 1, for $x \in F(\mathcal{O}, \mathbb{Q})$ and $t \in \mathcal{O}$,

$$(2) \quad \begin{aligned} W(\xi_x)(t) &\stackrel{(1)}{=} \sum_{r \in \mathcal{O}} x(r) \sum_{p \in \mathcal{O}} D_{r,p} \Delta_{\{p, M \setminus p\}}(t) \\ &= \sum_{r \in \mathcal{O}} x(r) \sum_{p \in \mathcal{O}} D_{r,p} B_{p,t} = \sum_{r \in \mathcal{O}} x(r) (DB)_{r,t} = x(t). \end{aligned}$$

For every $\alpha \in \mathcal{P} \setminus \mathcal{P}_2$ define the function in $F(\mathcal{P}, \mathbb{Q})$,

$$\zeta_\alpha := \mathbb{1}_\alpha - \xi_{\Delta_\alpha}.$$

Recall that for a partition $\alpha \in \mathcal{P}$, the function Δ_α is in $F(\mathcal{O}, \mathbb{Q})$. Using this equality, for $\alpha \in \mathcal{P}$,

$$(3) \quad W(\zeta_\alpha) \stackrel{(1)}{=} \Delta_\alpha - W(\xi_{\Delta_\alpha}) \stackrel{(2)}{=} \Delta_\alpha - \Delta_\alpha = 0.$$

Consider the subspace V_0 of $F(\mathcal{P}, \mathbb{Q})$ of those functions that take zero values on the partitions in $\mathcal{P} \setminus \mathcal{P}_2$,

$$V_0 := \{\eta \in F(\mathcal{P}, \mathbb{Q}) \mid \forall \alpha \in \mathcal{P} \setminus \mathcal{P}_2, \eta(\alpha) = 0\}.$$

The subspace V_0 is the image of the canonical embedding of $F(\mathcal{P}_2, \mathbb{Q})$ into $F(\mathcal{P}, \mathbb{Q})$.

Proposition 4. *If $m \geq 5$ or $m = 3$, then $F(\mathcal{P}, \mathbb{Q}) = V_0 \oplus \text{Ker } W$.*

Proof. From eq. (2), the map $\xi_x \in F(\mathcal{P}, \mathbb{Q})$ is a pre-image of a map $x \in F(\mathcal{O}, \mathbb{Q})$ under the map W , and hence $W : F(\mathcal{P}, \mathbb{Q}) \rightarrow F(\mathcal{O}, \mathbb{Q})$ is onto. The dimension of the kernel of W is equal to $|\mathcal{P}| - |\mathcal{O}| = |\mathcal{P}| - |\mathcal{P}_2| = |\mathcal{P} \setminus \mathcal{P}_2|$, which is true for $m \neq 4$. Obviously, the maps ζ_α for $\alpha \in \mathcal{P} \setminus \mathcal{P}_2$, are linearly independent over \mathbb{Q} and thus form a basis of $\text{Ker } W$: see eq. (3). The dimension of V_0 is equal to $|\mathcal{P}_2|$. Also, $\text{Ker } W \cap V_0 = \{0\}$. Therefore, $F(\mathcal{P}, \mathbb{Q}) = V_0 \oplus \text{Ker } W$. \square

8. PROOF OF THE MAIN THEOREM

Before starting to prove the main theorem, let us prove several necessary equalities.

For $g \in \mathfrak{S}(M)$ and $p = \{i, j\} \in \mathcal{O}$, the value $g(\Delta_\alpha)(p) = \Delta_\alpha(g^{-1}(p))$ is 0 if $g^{-1}(i)$ and $g^{-1}(j)$ belong to the same class in α , and the value is 1 otherwise. Obviously, $g^{-1}(i)$ and $g^{-1}(j)$ are in the same class of α if and only if i and j are in the same class of $g(\alpha)$. Thus we have the equality

$$(4) \quad \Delta_{g(\alpha)} = g(\Delta_\alpha).$$

For $g \in \mathfrak{S}(M)$, for $\eta \in F(\mathcal{P}, \mathbb{Q})$ and $p \in \mathcal{O}$,

$$\begin{aligned} W(g(\eta))(p) &= \sum_{\alpha \in \mathcal{P}} g(\eta)(\alpha) \Delta_{\alpha}(p) = \sum_{\alpha \in \mathcal{P}} \eta(g^{-1}(\alpha)) \Delta_{\alpha}(p) \\ (5) \quad &= \sum_{\beta \in \mathcal{P}} \eta(\beta) \Delta_{g(\beta)}(p) \stackrel{(4)}{=} \sum_{\beta \in \mathcal{P}} \eta(\beta) \Delta_{\beta}(g^{-1}(p)) = W(\eta)(g^{-1}(p)). \end{aligned}$$

For $g \in \mathfrak{S}(M)$ and for all $\beta \in \mathcal{P}$, the value $g(\mathbb{1}_{\alpha})(\beta) = \mathbb{1}_{\alpha}(g^{-1}(\beta))$ is 1, if $g(\alpha) = \beta$, and is 0 otherwise. Hence we have the equality

$$(6) \quad g(\mathbb{1}_{\alpha}) = \mathbb{1}_{g(\alpha)}.$$

For $g \in \mathfrak{S}(M)$, for $x \in F(\mathcal{O}, \mathbb{Q})$,

$$\begin{aligned} g(\xi_x) &= \sum_{r \in \mathcal{O}} x(r) \sum_{p \in \mathcal{O}} D_{r,p} \mathbb{1}_{\{g(p), M \setminus g(p)\}} = \sum_{r \in \mathcal{O}} x(r) \sum_{g^{-1}(p) \in \mathcal{O}} D_{r, g^{-1}(p)} \mathbb{1}_{\{p, M \setminus p\}} \\ (7) \quad &= \sum_{r \in \mathcal{O}} x(r) \sum_{p \in \mathcal{O}} D_{g(r), p} \mathbb{1}_{\{p, M \setminus p\}} = \sum_{g^{-1}(r) \in \mathcal{O}} x(g^{-1}(r)) \sum_{p \in \mathcal{O}} D_{r, p} \mathbb{1}_{\{p, M \setminus p\}} \\ &= \sum_{r \in \mathcal{O}} g(x)(r) \sum_{p \in \mathcal{O}} D_{r, p} \mathbb{1}_{\{p, M \setminus p\}} = \xi_{g(x)}. \end{aligned}$$

For $g \in \mathfrak{S}(M)$ and $\alpha \in \mathcal{P}$,

$$(8) \quad g(\zeta_{\alpha}) = g(\mathbb{1}_{g(\alpha)}) - g(\xi_{\Delta_{\alpha}}) = \mathbb{1}_{g(\alpha)} - \xi_{\Delta_{g(\alpha)}} = \zeta_{g(\alpha)},$$

where the equality in the middle holds due to eq. (4), eq. (6) and eq. (7).

Lemma 2. *If $\eta_0 \in \text{Ker } W$ and $\eta_1 \in V_0$, then the equalities hold,*

$$\begin{aligned} \text{Stab}(\eta_0 + \eta_1) &= \text{Stab}(\eta_0) \cap \text{Stab}(\eta_1), \\ \text{Stab}_W(\eta_0 + \eta_1) &= \text{Stab}_W(\eta_1) = \text{Stab}(\eta_1). \end{aligned}$$

Proof. We first show that the spaces $\text{Ker } W$ and V_0 are invariant under the action of $\mathfrak{S}(M)$. Indeed, for $g \in \mathfrak{S}(M)$, if $\eta \in \text{Ker } W$, then for all $p \in \mathcal{O}$,

$$W(g(\eta))(p) \stackrel{(5)}{=} W(\eta)(g^{-1}(p)) = 0,$$

and hence $g(\eta) \in \text{Ker } W$. If $\eta \in V_0$, then for all $\alpha \in \mathcal{P} \setminus \mathcal{P}_2$, $g(\eta)(\alpha) = \eta(g^{-1}(\alpha)) = 0$, and thus $g(\eta) \in V_0$.

Now we prove the first equality. If $g \in \text{Stab}(\eta_0) \cap \text{Stab}(\eta_1)$, then $g(\eta_0) = \eta_0$ and $g(\eta_1) = \eta_1$. Hence $g(\eta_0 + \eta_1) = g(\eta_0) + g(\eta_1) = \eta_0 + \eta_1$ and thus $g \in \text{Stab}(\eta_0 + \eta_1)$. Conversely, if $g \in \text{Stab}(\eta_0 + \eta_1)$, then $g(\eta_0 + \eta_1) = \eta_0 + \eta_1$. Since $g(\eta_0) \in \text{Ker } W$ and $g(\eta_1) \in V_2$, by the uniqueness of the decomposition (see Proposition 4) $g(\eta_0) = \eta_0$ and $g(\eta_1) = \eta_1$, which means $g \in \text{Stab}(\eta_0) \cap \text{Stab}(\eta_1)$. Therefore, $\text{Stab}(\eta_0) \cap \text{Stab}(\eta_1) = \text{Stab}(\eta_0 + \eta_1)$.

The second equality follows from the fact that for all $p \in \mathcal{O}$, $W(\eta_0 + \eta_1) = W(\eta_0) + W(\eta_1) = W(\eta_1)$ and for all $g \in \mathfrak{S}(M)$, $W(g(\eta_0 + \eta_1)) = W(g(\eta_0)) + W(g(\eta_1)) = W(g(\eta_1))$.

Finally, we prove the third equality. The restriction of W on the subspace V_0 is a bijection by Proposition 4. If $g \in \text{Stab}_W(\eta_1)$, then $W(g(\eta_1)) = W(\eta_1)$. The map $g(\eta_1)$ is in V_0 . Hence, applying W^{-1} to both sides of equality, we get $g(\eta_1) = \eta_1$ and thus $g \in \text{Stab}(\eta_1)$. Since $\text{Stab}(\eta_1) \leq \text{Stab}_W(\eta_1) \leq \text{Stab}(\eta_1)$, we get the third equality in the statement. \square

Recall that \mathcal{P}_2 is a set of partitions of the form $\{p, M \setminus p\}$, $p \in \mathcal{O}$. Define the map $\mathbb{1}_{\mathcal{P}_2} \in F(\mathcal{P}, \mathbb{Q})$,

$$\mathbb{1}_{\mathcal{P}_2} = \sum_{\alpha \in \mathcal{P}_2} \mathbb{1}_\alpha.$$

Lemma 3. *Let $\eta \in F(\mathcal{P}, \mathbb{Q})$. For all $c \in \mathbb{Q}$,*

$$\begin{aligned} \text{Stab}(\eta) &= \text{Stab}(\eta + c\mathbb{1}_{\mathcal{P}_2}), \\ \text{Stab}_W(\eta) &= \text{Stab}_W(\eta + c\mathbb{1}_{\mathcal{P}_2}). \end{aligned}$$

Proof. For all $g \in \mathfrak{S}(M)$,

$$g(\mathbb{1}_{\mathcal{P}_2}) = \sum_{\alpha \in \mathcal{P}_2} g(\mathbb{1}_\alpha) \stackrel{(6)}{=} \sum_{\alpha \in \mathcal{P}_2} \mathbb{1}_{g(\alpha)} = \sum_{g^{-1}(\alpha) \in \mathcal{P}_2} \mathbb{1}_\alpha = \mathbb{1}_{\mathcal{P}_2}.$$

We now prove the second equality of the statement. If $g \in \text{Stab}_W(\eta)$, then

$$W(g(\eta + c\mathbb{1}_{\mathcal{P}_2})) = W(g(\eta)) + W(cg(\mathbb{1}_{\mathcal{P}_2})) = W(\eta) + W(c\mathbb{1}_{\mathcal{P}_2}) = W(\eta + c\mathbb{1}_{\mathcal{P}_2}).$$

Hence $g \in \text{Stab}_W(\eta + c\mathbb{1}_{\mathcal{P}_2})$ and therefore $\text{Stab}_W(\eta) \subseteq \text{Stab}_W(\eta + c\mathbb{1}_{\mathcal{P}_2})$. From this, $\text{Stab}_W(\eta + c\mathbb{1}_{\mathcal{P}_2}) \subseteq \text{Stab}_W((\eta + c\mathbb{1}_{\mathcal{P}_2}) + (-c)\mathbb{1}_{\mathcal{P}_2}) = \text{Stab}_W(\eta)$. The first equality is proven in the same way. \square

Now we are ready to prove the main theorem of the paper.

Proof of Theorem 1. Part (i). Let $\lambda \in F(M, A^n)$ be an encoding map of the code C . From Proposition 3, we have to show that $\text{Iso}(C) = \text{Stab}_W(\eta_\lambda)$ is closed under the action on \mathcal{P}_2 . Since the bijection $\mathcal{O} \rightarrow \mathcal{P}_2$, $p \mapsto \{p, M \setminus p\}$ preserves the action of the group $\mathfrak{S}(M)$, we have to show that $\text{Stab}_W(\eta_\lambda)$ is closed under the action on \mathcal{O} . If $g \in \mathfrak{S}(M)$ preserves the orbits of $\text{Stab}_W(\eta_\lambda)$ on \mathcal{O} , then so does g^{-1} , and for all $p \in \mathcal{O}$,

$$W(g(\eta_\lambda))(p) \stackrel{(5)}{=} W(\eta_\lambda)(g^{-1}(p)) = W(\eta_\lambda)(p).$$

Hence $g \in \text{Stab}_W(\eta_\lambda)$, which means that $\text{Stab}_W(\eta_\lambda)$ is closed under the action on \mathcal{O} .

Part (ii). Let $\lambda \in F(M, A^n)$ be an encoding map of the code C . From Proposition 4, there exists the unique decomposition of the multiplicity function $\eta_\lambda \in F(\mathcal{P}, \mathbb{Q})$ into the sum of two maps $\eta_0 \in \text{Ker } W$ and $\eta_1 \in V_0$ with $\eta_\lambda = \eta_0 + \eta_1$.

From Proposition 3, $\text{Stab}(\eta_\lambda) = \text{Mon}(C)$ and $\text{Stab}_W(\eta_\lambda) = \text{Iso}(C)$. From Lemma 2, $\text{Stab}(\eta_\lambda) = \text{Stab}(\eta_0) \cap \text{Stab}_W(\eta_\lambda)$. Finally, we have $\text{Mon}(C) = \text{Stab}(\eta_0) \cap \text{Iso}(C)$.

Let us prove that $\text{Stab}(\eta_0)$ is closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$. Let $g \in \mathfrak{S}(M)$ preserve the orbits of $\text{Stab}(\eta_0)$ acting on $\mathcal{P} \setminus \mathcal{P}_2$. This means that $\eta_0(\alpha) = \eta_0(g(\alpha))$ for all $\alpha \in \mathcal{P} \setminus \mathcal{P}_2$. Consider the expansion of the map η_0 in the basis ζ_β , $\beta \in \mathcal{P} \setminus \mathcal{P}_2$,

$$\eta_0 = \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(\beta) \zeta_\beta.$$

For $\alpha \in \mathcal{P}$,

$$\begin{aligned} g^{-1}(\eta_0)(\alpha) &= \eta_0(g(\alpha)) = \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(\beta) \zeta_\beta(g(\alpha)) \stackrel{(8)}{=} \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(\beta) \zeta_{g^{-1}(\beta)}(\alpha) \\ &= \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(g(\beta)) \zeta_\beta(\alpha) = \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(\beta) \zeta_\beta(\alpha) = \eta_0(\alpha). \end{aligned}$$

Hence $g \in \text{Stab}(\eta_0)$, and therefore $\text{Stab}(\eta_0)$ is closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$.

Part (iii). Let $x \in F(\mathcal{O}, \mathbb{Q})$ be a function that takes equal values on each orbit and different values on different orbits of H_2 acting on \mathcal{O} . From eq. (2) and eq. (7), $\text{Stab}_W(\xi_x) = \{g \in \mathfrak{S}(M) \mid W(g(\xi_x)) = W(\xi_x)\} = \{g \in \mathfrak{S}(M) \mid g(x) = x\}$. For every $g \in H_2$, $g(x) = x$ and thus $H_2 \subseteq \text{Stab}_W(\xi_x)$. Conversely, if $g \in \text{Stab}_W(\xi_x)$, then $g(x) = x$ and thus g preserves the orbits of H_2 . As in the proof of part (i), the group H_2 is closed under the action on \mathcal{O} , and hence $g \in H_2$. Finally, $H_2 = \text{Stab}_W(\xi_x)$.

Let $\{X_1, \dots, X_t\}$ be the set of orbits of H_1 acting on the set $\mathcal{P} \setminus \mathcal{P}_2$. Let $c_1, \dots, c_t \in \mathbb{Q}$ be different nonnegative numbers and define the map

$$\eta_0 = \sum_{i=1}^t c_i \sum_{\alpha \in X_i} \zeta_\alpha.$$

For all $g \in H_1$,

$$g(\eta_0) = \sum_{i=1}^t c_i \sum_{\alpha \in X_i} g(\zeta_\alpha) \stackrel{(8)}{=} \sum_{i=1}^t c_i \sum_{\alpha \in X_i} \zeta_{g(\alpha)} = \sum_{i=1}^t c_i \sum_{g^{-1}(\alpha) \in X_i} \zeta_\alpha = \eta_0,$$

and thus $H_1 \leq \text{Stab}(\eta_0)$. Conversely, if $g \in \text{Stab}(\eta_0)$, then, for every $i \in \{1, \dots, t\}$ and every $\beta \in X_i$, $\eta_0(g^{-1}(\beta)) = g(\eta_0)(\beta) = \eta_0(\beta) = c_i$. Hence $g^{-1}(\beta) \in X_i$ and thus $g^{-1}(X_i) = X_i$. Since H_1 is closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$, we have $g^{-1} \in H_1$ and thus $g \in H_1$. Hence $H_1 = \text{Stab}(\eta_0)$.

Since $\eta_0 \in \text{Ker } W$ and $\xi_x \in V_0$, from Lemma 2, $\text{Stab}_W(\eta_0 + \xi_x) = \text{Stab}_W(\xi_x) = H_2$ and $\text{Stab}(\eta_0 + \xi_x) = \text{Stab}(\eta_0) \cap \text{Stab}_W(\xi_x) = H_1 \cap H_2$.

There exist two nonnegative integers c, c' such that $c'(\eta_0 + \xi_x) + c\mathbb{1}_{\mathcal{P}_2}$ takes positive integer values. From Lemma 3, $\text{Stab}_W(c'(\eta_0 + \xi_x) + c\mathbb{1}_{\mathcal{P}_2}) = \text{Stab}_W(c'(\eta_0 + \xi_x)) = \text{Stab}_W(\eta_0 + \xi_x) = H_2$ and $\text{Stab}(c'(\eta_0 + \xi_x) + c\mathbb{1}_{\mathcal{P}_2}) = \text{Stab}(c'(\eta_0 + \xi_x)) = \text{Stab}(\eta_0 + \xi_x) = H_1 \cap H_2$.

From Proposition 1, there exists an encoding map $\lambda : M \rightarrow A^n$ such that $\eta_\lambda = c'(\eta_0 + \xi_x) + c\mathbb{1}_{\mathcal{P}_2}$. Define $C = \lambda(M)$. By Proposition 3, $\text{Iso}(C) = \text{Stab}_W(\eta_\lambda) = H_2$ and $\text{Mon}(C) = \text{Stab}(\eta_\lambda) = H_1 \cap H_2 = H_1 \cap \text{Iso}(C)$. \square

APPENDIX A. CODES WITH 4 ELEMENTS

There are two main reasons why the general approach of the paper fails for $m = 4$. The first reason is that for $m = 4$ the sets \mathcal{P}_2 and \mathcal{O} have 3 and 6 elements correspondingly, whereas for $m \geq 5$ or $m = 3$, $|\mathcal{P}_2| = |\mathcal{O}| = \frac{m(m-1)}{2}$, which is crucial in several places in the proof. The second reason is that the matrix B is not invertible and the matrix D is not defined.

However, if $m = 4$ and $q \geq 3$, we still can use the basic idea and an analogue of Theorem 1 holds. For this, let us make several changes in the text of the paper.

Replace \mathcal{P}_2 with

$$\mathcal{P}'_2 := \left\{ \{ \{i\}, \{j\}, \{M \setminus \{i, j\}\} \} \mid \{i, j\} \subset M \right\}.$$

The set \mathcal{P}'_2 is well-defined since each of its elements has 3 classes, which is not greater than q .

Replace the matrices B and D with B' and D' , for $p, t \in \mathcal{O}$, where

$$B'_{p,t} := \begin{cases} 1, & \text{if } |p \cap t| \neq 0; \\ 0, & \text{if } |p \cap t| = 0. \end{cases} \quad D'_{p,t} := \begin{cases} \frac{1}{5}, & \text{if } |p \cap t| \neq 0; \\ -\frac{4}{5}, & \text{if } |p \cap t| = 0. \end{cases}$$

And replace the map ξ_x with

$$\xi'_x := \sum_{p=\{i,j\} \in \mathcal{O}} \sum_{r \in \mathcal{O}} D'_{r,p} x(r) \mathbb{1}_{\{\{i\}, \{j\}, M \setminus p\}}.$$

In such a way $|\mathcal{P}'_2| = |\mathcal{O}|$ and the bijection $\mathcal{P}'_2 \rightarrow \mathcal{O}, \{ \{i\}, \{j\}, M \setminus \{i, j\} \} \mapsto \{i, j\}$ preserves the action of the group $\mathfrak{S}(M)$. Also, B' is invertible and $B'D' = D'B' = I$, where I is the 6×6 identity matrix.

One can verify that all the statement, equalities and proofs remain correct with these changes.

Consider the case $m = 4$ and $q = 2$. The set \mathcal{P} contains 8 partitions and the set \mathcal{O} contains 6 pairs. Fixing bases in $F(\mathcal{P}, \mathbb{Q})$ and $F(\mathcal{O}, \mathbb{Q})$, look at the \mathbb{Q} -linear map W as the following 6×8 matrix over \mathbb{Q} :

$$W = \left(\begin{array}{c|ccc|ccc} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array} \right).$$

The vertical lines separate the columns labeled by partitions from three different orbits under the action of \mathfrak{S}_4 on the set \mathcal{P} .

Proposition 5. *Let C be a binary code with 4 codewords. The groups $\text{Iso}(C) \leq \mathfrak{S}_4$ and $\text{Mon}(C) \leq \mathfrak{S}_4$ are equal and are closed under the action on \mathcal{O} . For every subgroup $H \leq \mathfrak{S}_4$ that is closed under the action on \mathcal{O} , there exists a binary code C with 4 codewords such that $\text{Iso}(C) = \text{Mon}(C) = H$.*

Proof. It is easy to calculate that $\text{Ker } W$ is a subspace of dimension 2 generated by $(1, 0, 0, 0, 0, 0, 0, 0)^T$ and $(0, 1, 1, 1, 1, -1, -1, -1)^T$. Note that $\text{Ker } W$ is invariant under the action of \mathfrak{S}_4 .

Let $\lambda : M \rightarrow \{0, 1\}^n$ be an encoding map of C . Assume that $W(\eta_\lambda) = W(\eta_{g\lambda})$, or equivalently, $\eta_\lambda - \eta_{g\lambda} \in \text{Ker } W$, for some $g \in \mathfrak{S}_4$. In the proof of Proposition 3 we showed that $\eta_{g\lambda} = g(\eta_\lambda)$. Then, $24(\eta_\lambda - \eta_{g\lambda}) = \sum_{h \in \mathfrak{S}_4} h(\eta_\lambda - g(\eta_\lambda)) = \sum_{h \in \mathfrak{S}_4} h(\eta_\lambda) - \sum_{h \in \mathfrak{S}_4} h(\eta_\lambda) = 0$. Hence, $W(\eta_\lambda) = W(\eta_{g\lambda})$ implies $\eta_\lambda = \eta_{g\lambda}$ for all $g \in \mathfrak{S}_4$. By Proposition 2 and Proposition 3, $\text{Iso}(C) = \text{Mon}(C)$.

The fact that the groups $\text{Iso}(C) = \text{Mon}(C)$ are closed under the action on \mathcal{O} is proven in the same way as Theorem 1 (i).

To prove the last statement, for each subgroup of \mathfrak{S}_4 closed under the action on \mathcal{O} we give a construction of the code. Any binary code of cardinality 4, up to a

monomial equivalence, has the following form,

$$\begin{array}{c|cccc|ccc} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{array},$$

where x_1, \dots, x_8 are nonnegative integers; see Example 2 for more details. There exist 7, up to an automorphism, non-equivalent subgroups in \mathfrak{S}_4 that are closed under the action on \mathcal{O} . The groups and corresponding multiplicity functions of the corresponding codes are given in the following table.

Group	$\eta_\lambda = (x_1, \dots, x_8)$
$\{e\}$	$(0, 1, 2, 3, 4, 0, 0, 0)$
$\langle(1, 2)\rangle \cong \mathfrak{S}_2$	$(0, 1, 1, 2, 3, 0, 0, 0)$
$\langle(1, 2), (1, 2, 3)\rangle \cong \mathfrak{S}_3$	$(0, 1, 1, 1, 2, 0, 0, 0)$
$\langle(1, 2), (3, 4)\rangle \cong K_4$	$(0, 1, 1, 2, 2, 0, 0, 0)$
$\langle(1, 2)(3, 4), (1, 3)(2, 4)\rangle \cong K_4$	$(0, 0, 0, 0, 0, 2, 1, 0)$
$\langle(1, 2, 3, 4), (1, 3)\rangle \cong D_8$	$(0, 0, 0, 0, 0, 1, 0, 1)$
\mathfrak{S}_4	$(0, 1, 1, 1, 1, 0, 0, 0)$

□

REFERENCES

- [1] S. V. Avgustinovich and F. I. Solov'eva. To the metrical rigidity of binary codes. *Problems of Information Transmission*, 39(2):178–183, Apr. 2003.
- [2] P. G. A. Bonneau. *Codes et combinatoire*. PhD thesis, Université Pierre et Marie Curie, Paris, 1984.
- [3] I. Constantinescu and W. Heise. On the concept of code-isomorphy. *Journal of Geometry*, 57(1-2):63–69, 1996.
- [4] H. Q. Dinh and S. R. López-Permouth. On the equivalence of codes over rings and modules. *Finite Fields and Their Applications*, 10(4):615 – 625, 2004.
- [5] J. D. Dixon and B. Mortimer. *Permutation Groups*, volume 163 of *Graduate texts in mathematics*. Springer, 1996.
- [6] M. Greferath, A. Nechaev, and R. Wisbauer. Finite quasi-Frobenius modules and linear codes. *Journal of Algebra and Its Applications*, 03(03):247–272, 2004.
- [7] D. I. Kovalevskaya. On metric rigidity for some classes of codes. *Problems of Information Transmission*, 47(1):15–27, Mar. 2011.
- [8] F. J. MacWilliams. *Combinatorial Properties of Elementary Abelian Groups*. Ph.D. thesis, Radcliffe College, 1962.
- [9] F. Solov'eva, T. Honold, S. Avgustinovich, and W. Heise. On the extendability of code isometries. *Journal of Geometry*, 61(1-2):2–16, 1998.
- [10] H. Wielandt. *Permutation groups through invariant relations and invariant functions*. Dept. of Mathematics, Ohio State University, Columbus, 1969.
- [11] J. A. Wood. Isometry Groups of Additive Codes. Paper presented at AMS meeting in October 2015, Loyola University, Chicago IL.
- [12] J. A. Wood. The structure of linear codes of constant weight. *Electronic Notes in Discrete Mathematics*, 6:287 –296, 2001. WCC2001, International Workshop on Coding and Cryptography.
- [13] J. A. Wood. Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. In *Codes over rings*, volume 6 of *Ser. Coding Theory Cryptol.*, pages 124–190. World Sci. Publ., Hackensack, NJ, 2009.
- [14] J. Xu. *On closures of finite permutation groups*. PhD thesis, The University of Western Australia, 2005.

E-mail address: `dyshko@univ-tln.fr`